NAME

pki --gen - Generate a new RSA or ECDSA private key

SYNOPSIS

pki --gen[**--type** *type*] [**--size** *bits*] [**--safe-primes**] [**--shares** *n*] [**--threshold** *l*] [**--outform** *encoding*] [**--debug** *level*]

pki --gen--options *file*

pki --gen-h | **--help**

DESCRIPTION

This sub-command of **pki**(1) is used to generate a new RSA or ECDSA private key.

OPTIONS

-h, --help

Print usage information with a summary of the available options.

-v, --debug *level*

Set debug level, default: 1.

-+, --options *file*

Read command line options from *file*.

-t, --type *type*

Type of key to generate. Either *rsa*, *ecdsa*, *ed25519*, *ed448* or *bliss*, defaults to *rsa*.

-s, --size *bits*

Key length in bits. Defaults to 2048 for *rsa* and 384 for *ecdsa*. For *ecdsa* only three values are currently supported: 256, 384 and 521.

-p, --safe-primes

Generate RSA safe primes.

-f, --outform *encoding*

Encoding of the generated private key. Either *der* (ASN.1 DER) or *pem* (Base64 PEM), defaults to *der*.

RSA Threshold Cryptography

-n, --shares <*n*>

Number of private RSA key shares.

-l, --threshold <*l*>
Minimum number of participating RSA key shares.

PROBLEMS ON HOSTS WITH LOW ENTROPY

If the *gmp* plugin is used to generate RSA private keys the key material is read from */dev/random* (via the *random* plugin). Therefore, the command may block if the system's entropy pool is empty. To avoid this, either use a hardware random number generator to feed */dev/random* or use OpenSSL (via the *openssl* plugin or the command line) which is not as strict in regards to the quality of the key material (it reads from */dev/urandom* if necessary). It is also possible to configure the devices used by the *random* plugin in **strongswan.conf**(5). Setting **libstrongswan.plugins.random.random** to */dev/urandom* forces the plugin to treat bytes read from */dev/urandom* as high grade random data, thus avoiding the blocking. Of course, this doesn't change the fact that the key material generated this way is of lower quality.

EXAMPLES

pki --gen --size 3072 > rsa_key.der
Generates a 3072-bit RSA private key.

pki --gen --type ecdsa --size 256 > ecdsa_key.der
Generates a 256-bit ECDSA private key.

SEE ALSO

pki(1)